Design and Implementation of a Security Detection System Based on Smart Automated Architecture

DAUDA MUSTAPHA[1], UMAR SALISU LAWAL[2], USMAN OMEIZA AHMED[3], BOTSON ISHAYA CHOLLOM[4]

[1,2,3,4]*Department of Electrical/Electronic Engineering Technology,Federal Polytechnic Nasarawa, Nasarawa State, Nigeria*

Abstract- ***Since electronic and communication technologies are becoming more and more popular, the number of digital applications in our modern society is growing every day. The past few decades have seen tremendous advancements in the creation of security systems to prevent security breaches. In the context of technological advancement, traditional security systems are currently experiencing significant changes. Deploying advanced technology to secure contemporary human societies has become simpler with the rise of new security architectures that use smart and intelligent connectivity. In order to close a gap in the current systems, this study focuses on the development and deployment of a wireless intrusion detection smart security system. The security gadget is characterised by its portability, affordability, intelligence, and ability to efficiently carry out its intended purpose of monitoring activity at the installed area. By sending a voice call to the homeowner's authorised phone number and setting off a security breach detection alarm, the security device uses a combination of embedded hardware and software to identify security breaches by an intruder. Positive findings emerged from the preliminary test conducted, such that the system can remotely alert the user of an intruder, even if they are not online, by using a GSM module to send a voice call to them.***

Indexed Terms- ***Automated Architecture, Electronic, Intelligent, Internet, Security, Smart System***

I. INTRODUCTION

Security cannot be ignored anymore, and the creation of a comprehensive security concept is 1crucial given the growing demand to combine security services that were previously supplied by separate subsystems. The strengthening of modern household security architecture has become very important, considering the fact that there are growing threats to lives and properties in our societies. Advancement in modern security development is based on the digitization of security detection systems through the application of Internet of Things (IoT) technology [1-3]. IoT systems are software-based systems integrated with sensors and actuators to perform intelligent functions through the exchange of information or data over a given network and communication devices. Modern security architectural development uses IoT technology to automate domestic appliances for the enhancement of home security. The idea of a smart home brought about smart security engagement, incorporating intelligent systems. In Fig. 1, the stage involved in the design of smart concepts for home security detection. The advancement of information and communication technology (ICT) and the advent of smart energy infrastructure have shaped the security architecture of the entire world. The incursion of new smart devices with potential capability to connect to the internet has changed the global efforts in the development of embedded sensors, electronics, software and connectivity is called the Internet of Things (IoT). Recently, IoT technology has developed with tremendous capabilities through cloud computing solutions.

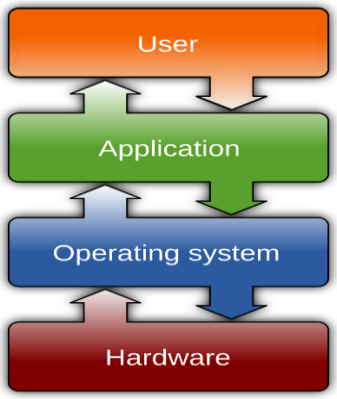

Fig. 1: Stages involved in the design of smart concepts for home security detection

IoT systems have created a paradigm shift, especially from functionality to connectivity and data-driven decision making for the interconnectivity of electronic devices used for different applications. Smart security concept through the application of IoT schemes has created integrated links between virtual and the real-world experience in different aspects of human development. Before the development of IoT technologies, electronic calculators and traditional computer systems were used to carry out sophisticated computations. Furthermore, virtual communication was extremely challenging to do. The development of IoT technology has made it easier to link devices, perform calculations, and communicate in real time, whether in person or virtually. Among other technologies, Bluetooth, GSM, and GPRS have made it easier for people to communicate and share data. They may also control one another via the internet for data and security management. In the context of IoT applications, data and security management are also provided by the embedded hardware, software, or sensor. Since the IoT connects people and things and makes computing possible from anywhere at any time, it can be compared to universal computing.

There are several uses of IoT, including smart energy and smart homes. Presently, smart devices are now safer and more automated, which facilitates communication. Recent developments indicate that security is a difficult and developing area of study. By creating effective and efficient methods and technologies to preserve data integrity and to monitor and prevent unauthorised access to a protected environment, security plays a significant and crucial role in protecting devices, data, and networks against intrusions. IoT security is a new and developing subject of study that focuses on safeguarding the networks and linked devices that are part of the IoT. Advanced technologies in the IoT have the potential to completely transform our lives and create a security system that an authorized user may monitor and control from any location. The existence of smart devices has created a greater sense of comfort in communication between people and devices. The focus of this study is on the design and development of a smart security alert system based on communication technologies and wireless protocols for mobile phone voice calls through an IoT technology.

II. LITERATURE REVIEW

Many facts have been established in research articles based on the use of IoT, wireless communication, smart security technologies and microcontroller integration in the field of security detection via smart automated architecture [4-8]. In order to link devices and provide access and control for the delivery of necessary services, smart technologies use information and communication technology in conjunction with technical electronic devices. An intelligent idea gives technologies a new look that is completely distinct from their traditional counterparts. Sensing and control systems are among the integrated schemes and technologies that smart technologies make use of. In order to optimise performance metrics, smart technologies investigate a smart environment as an intelligent agent that can evaluate the state of various objects. Security detection is one of the performance metrics that smart technologies may optimise [9]. From the standpoint of contemporary technology, the automation of a system or gadget does not always imply intelligence. Automation and intelligence came about as a result of the goal to create a safe home structure for simple detection. Automation allows for the creation of self-regulating and operating devices that are influenced by external environmental factors. A smart system, on the other hand, can gather environmental data, store it, and use it to make decisions without the user's help. The architectures used by various smart systems vary according to the operational intelligence requirements. As shown in Fig. 2, smart buildings, in particular, exploit a variety of important concepts.

The way devices connect, how and where sensor and appliance usage data is saved, how this data is processed, and how the user can interact with the devices all influence the architecture of a smart home. Smart home security systems that connect sensors and actuators to a microcontroller for data collection have been studied [10]. The intended action was achieved by using ZigBee technology to communicate environmental data from sensors to a microcontroller. Cook et al. [11] built a home automation system using a microprocessor, motion sensors and actuators using ZigBee wireless communication technology. A cloud-based architecture was utilised in the work by Zhou et al. [12] to create a home-based security infrastructure for smart home device management and security

intrusion detection. The performance of a smart home gateway technological device and the hardware requirements were investigated in Hosek et al. [13]. In essence, the paper offers ways to capitalise on increased processing power and scalable design while simultaneously improving availability, dependability and security.

Fig. 2: Elements of a smart building [14]

The IoT, according to Kodali et al. [15], is a system that remotely connects and monitors actual objects to the internet. The study highlighted that the advantage of an IoT system over other existing systems is that the user can receive the status and alerts sent by the Wi-Fi-connected microcontroller-managed system on their phone from any distance. The security system implemented in the work is that if any kind of human movement is detected close to the authorized user's home entrance, the system not only sounds an alarm but also sends an alert via an internet call. If the owner determines that the visitor is an unexpected visitor, the user can take certain desirable actions. A study on the deployment of wireless control systems and accessibility in a home setting for individuals who have been verified alone [16]. Motion detection and image capture are accomplished via a PIR motion sensor and a camera module, respectively. To notify neighbours when an intruder is spotted, a voice alert system is also incorporated. The system recognises the visitor, takes a picture, and automatically sends the owner a message with the picture. Every time someone tries to enter the residence, the system also produces speech output.

A smart home security system prototype that uses PIR sensors for intrusion detection was implemented by Shariq Suhail et al. [17]. This MCU board has outputs for a buzzer, LCD, LED strip, and GSM module. A Raspberry Pi 2 board is used to integrate a webcam that takes pictures when it detects motion, thereby sending SMS warnings and calls to the user's cell phone. A low-cost wireless home automation and security system based on a Microcontroller Unit (MCU) with integrated Wi-Fi connectivity has been implemented [18]. PIR motion sensors are installed at building entrances and are connected to an MCU's digital input-output pin with enabled Wi-Fi. The project uses Energia Integrated Development Environment (IDE) for the programming of the MCU, which allows the use of mobile phones without internet access to control IoT devices linked to the microcontroller. In Henkel et al. [19], a low-cost home security system with a real-time email alert system was implemented. The system makes use of a Raspberry Pi, a security camera and a PIR sensor. The system sends real-time emails to residents via the Internet. The intrusion detection logic of the system detects motion by comparing the PIR sensors' signal inputs with their past values.

An affordable Ethernet-based smart house system for tracking temperature, smoke, energy use, and trespassing are studied by Khan [20]. A microcontroller board was used in this system and the microcontroller is directly connected to the temperature, smoke, and PIR sensors. Through the use of Google speech recognition techniques, users can switch devices using a mobile app that establishes an Internet connection with the microcontroller. In a Bluetooth-based home automation system presented by Piyare et al. [21], an Arduino board with digital and analogue input/output ports that are connected to sensors. The system uses Bluetooth connectivity between the smartphone and the Arduino board in a range of 50 m or less within a concrete building. Behera et al. [22] used an Arduino board, Wi-Fi, and a PC home server to build and implement a real-time smart home automation system. Data was gathered using a PIR motion sensor and other electronic components. By identifying potential intruders and sounding a buzzer to notify the occupants, the PIR sensor also served as a security feature. Using a similar architecture, Howedi et al. [23] proposed a low-cost smart home system that utilizes an Arduino board,

PIR sensors, temperature sensors, a DC sensor, and servo motors to control windows and doors against security threats.

The control and monitoring module of the system was implemented using Arduino, and a basic Android application was developed. A Raspberry Pi microcontroller served as the key hub for Panwar et al. [24] implementation of a smart home automation system. A home automation system with intelligent task scheduling was created by Baraka et al. [25] using wired technology to connect light and switch modules to an Arduino microcontroller and wireless ZigBee to connect appliances. An Ethernet shield installed on the Arduino MCU facilitates a connection between the Arduino and an Android web application, which is then used to view suggested schedules and add, manage, and update devices remotely. It is therefore important to note that previous research on smart home security systems has used different architectures that emphasise the use of a variety of sensors and inexpensive hardware components such as Arduino and Raspberry Pi boards for home security detection. Therefore, this study utilizes a combination of different electronic components and an Arduino microcontroller for the implementation of a home security detection system based on an offline information sharing system. Additionally, the proposed security system is to accurately detect the intruder or visitor who enters through the entrance and to be managed remotely, alerting the user on a mobile phone.

Implementation and Methodology

The hardware requirements for the implementation of the security detection system involve the following components: Arduino Uno, PIR sensor, transistor, resistors, connecting wires and a buzzer. There is also a software requirement using Arduino Integrated Development Environment (IDE) to enable writing of code. A variety of sensors are used in the GSM-enabled home security system to identify various security threats. The microprocessor, which continuously checks the sensors' state, controls the entire system. The authorised SIM card in a mobile phone will receive a voice call from the sensor if it detects any intruder. Fig. 3 shows the system's design diagram. The circuit microcontroller maintains the authorised owner's mobile number in its EEPROM memory and is designed to use it in conjunction with the microcontroller's triggering unit. The PIR sensor serves as the system's motion detector due to its architecture. Using the PIR sensor, a motion detection of an intruder triggers the buzzer alert in addition to making a voice call to a designated mobile communication line. Until the reset switch is turned on to the pre-specified mobile number entered into the program, the alarm will continue to ring. The designed security alert system's operational flow is represented in Fig. 4.

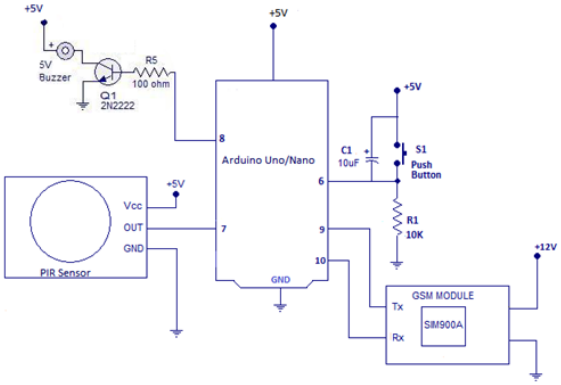

Fig. 3: Implementation circuit diagram of the home security detection system using Arduino and GSM module

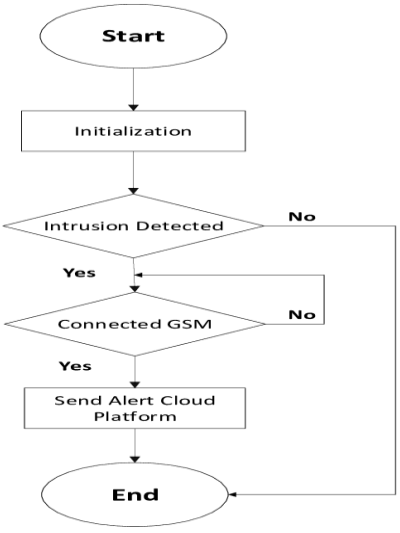

Fig. 4: Design and implementation of the operational flowchart of the system

III. RESULTS AND DISCUSSIONS

The home security system was designed to use a PIR sensor as a motion detector. Installed in a specific location, the system was designed to deliver the necessary voice call and sound an alarm when the

intruder circuit detected movement within the enclosed space, which raised the infrared radiation. For optimal sensitivity, the system's sensitivity can be changed using a variable resistor. In response to detecting movement or the presence of an intruder, the motion detector circuit will sound an alarm and make a voice call to the user's designated mobile communication line. An assessment of the system's performance in the form of a miniature smart home security system prototype and control over the automation of smart home devices served as the foundation for the study's findings. Numerous tests were conducted to evaluate the system's functionality, including the operation of the sensors. Experiments using the distance command are conducted by permitting various people to approach the device. When the system was turned on to carry out its designated task, it responded immediately and initialized. For the experiment, the device was installed on a security guard post. Based on the outcomes produced by the resulting system performance, the experimental results are examined. The purpose of the test is to ascertain whether the system can use the programmed SIM card to make a voice call to the authorised mobile phone. For the gadget to trigger as intended, a maximum distance of three meters was observed. Based on the test conducted, the device will actively start working at a distance of three meters, according to the results, by activating the intrusion detection warning through the buzzer and placing a voice call when required. The sound's strength tends to rise as one gets closer to the device. This indicates that the system can react appropriately. Furthermore, the following are some of the added advantages of the system designed and implemented in this study:

- A smartphone application serves as the user interface for this home security system. Numerous phones running various operating systems can access the system because it is platform-independent.
- A data connection on the user's phone is not required to run a home security system. Without a home WiFi connection, the system can function as expected.
- Considering that the system's launchpad is built to be able to make audio calls to numerous verified users. This raises the security system's chances.
- The technology is affordable since it makes use of the same set of motion sensors that can be used for home automation.
- A common flaw in many home security systems that causes needless embarrassment by setting off a security alarm is addressed by this system, which eliminates the need for the user to manually trigger an alarm and allows the alarm system to be operated independently. Moreover, this guarantees that the alarm can be turned off during the day and turned on at night when there is a higher likelihood of a security breach.

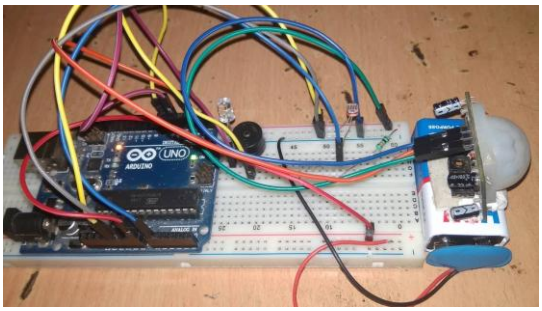

Fig. 4: Hardware implementation of a home security detection system using Arduino and GSM module

CONCLUSION AND RECOMMENDATIONS

The design and implementation of an Internet of Things-based intelligent security system featuring voice call notification is presented in this study. The required objective of a home security system has been met, and the suggested system offers the bare minimum of remote monitoring and home security. This security system has a higher likelihood of being used and a minimum delay during the voice call notification alert process. The results of the preliminary analysis are positive. The benefit of the suggested design system is that it can use a GSM module to call the user and tell them remotely of an intruder, even if they are not online. Although a call can only be successful when there is a strong network, a burglar alarm notice can be set off to make up for a mobile network outage. The developed system can be installed at the entrance of a home or workplace, or it can be used in smart homes. The suggested system's future functionality might be expanded to include further requirements for its operation, like a fingerprint sensor that would be used to cut off voice calls and the alerting sound when the device detects the legitimate occupant of the house. Since the homeowner can prevent incursions by receiving the proper notification, the

implementation of the compact home system was successfully tested and shown to be a dependable type of home security alert system. In comparison to the existing systems, it is both smaller and less expensive; yet, it was created in a way that allows for technical advancements to be made for a comprehensive result. The future upgrade may also involve the use of Wi-Fi Wi-Fi-enabled launchpad system with the capability to enable control from any part of the world.

ACKNOWLEDGEMENT

The authors strongly acknowledge the financial support from the Tertiary Education Trust Fund (TETFund) based on the Institution-Based Research (IBR) grant provided to the Federal Polytechnic Nasarawa (FPN).

REFERENCES

[1] Majeed, R., Abdullah, N. A., Ashraf, I., Zikria, Y. B., Mushtaq, M. F., & Umer, M. (2020). An intelligent, secure, and smart home automation system. *Scientific Programming*, *2020*(1), 4579291.

[2] Sayeduzzaman, M., Hasan, T., Nasser, A. A., & Negi, A. (2024). An internet of things-integrated home automation with smart security system. *Automated secure computing for next-generation systems*, 243-273.

[3] Suhaimi, A. F., Yaakob, N., Saad, S. A., Sidek, K. A., Elshaikh, M. E., Dafhalla, A. K., ... & Almashor, M. (2021, July). IoT based smart agriculture monitoring, automation and intrusion detection system. In *Journal of Physics: Conference Series* (Vol. 1962, No. 1, p. 012016). IOP Publishing.

[4] Ezugwu, A. E., Taiwo, O., Egwuche, O. S., Abualigah, L., Van Der Merwe, A., Pal, J., ... & Olusanya, M. O. (2025). Smart Homes of the Future. *Transactions on Emerging Telecommunications Technologies*, *36*(1), e70041.

[5] Rabbany, G., Miah, M. S., Ayan, M. B., Islam, M. R., Hossen, A., & Kabir, M. H. (2025, February). A design of IoT based secure smart lab. In *Data Science & Exploration in Artificial Intelligence: Proceedings of the First International Conference On Data Science & Exploration in Artificial Intelligence (CODE-AI 2024) Bangalore, India, 3rd-4th July, 2024 (Volume 1)* (p. 472). CRC Press.

[6] Jia, R., Jin, B., Jin, M., Zhou, Y., Konstantakopoulos, I. C., Zou, H., ... & Spanos, C. J. (2018). Design automation for smart building systems. *Proceedings of the IEEE*, *106*(9), 1680-1699.

[7] Netinant, P., Utsanok, T., Rukhiran, M., & Klongdee, S. (2024). Development and assessment of internet of things-driven smart home security and automation with voice commands. *IoT*, *5*(1), 79-99.

[8] Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. *Electronics*, *13*(16), 3343.

[9] Patel, P., & Shaikh, N. (2025, January). Smart home dashboard. In *AIP Conference Proceedings* (Vol. 3255, No. 1). AIP Publishing.

[10] Soliman, M., Abiodun, T., Hamouda, T., Zhou, J., & Lung, C. H. (2013, December). Smart home: Integrating internet of things with web services and cloud computing. In *2013 IEEE 5th international conference on cloud computing technology and science* (Vol. 2, pp. 317-320). IEEE.

[11] Cook, D. J., Crandall, A. S., Thomas, B. L., & Krishnan, N. C. (2012). CASAS: A smart home in a box. *Computer*, *46*(7), 62-69.

[12] Zhou, J., Leppanen, T., Harjula, E., Ylianttila, M., Ojala, T., Yu, C., ... & Yang, L. T. (2013, June). Cloudthings: A common architecture for integrating the internet of things with cloud computing. In *Proceedings of the 2013 IEEE 17th international conference on computer supported cooperative work in design (CSCWD)* (pp. 651-657). IEEE.

[13] Hosek, J., Masek, P., Kovac, D., Ries, M., & Kröpfl, F. (2014). IP home gateway as universal multi-purpose enabler for smart home services. *Elektrotech. Informationstechnik*, *131*(4-5), 123-128.

[14] Whaiduzzaman, M., Barros, A., Chanda, M., Barman, S., Sultana, T., Rahman, M. S., ... & Fidge, C. (2022). A review of emerging technologies for IoT-based smart cities. *Sensors*, *22*(23), 9271.

[15] Kodali, R. K., Jain, V., Bose, S., & Boppana, L. (2016, April). IoT based smart security and

home automation system. In *2016 international conference on computing, communication and automation (ICCCA)* (pp. 1286-1289). IEEE.

[16] Anwar, S., & Kishore, D. (2016). IOT based smart home security system with alert and door access control using smart phone. *International Journal of Engineering Research & Technology (IJERT)*, *5*(12), 504-509.

[17] ShariqSuhail, M., ViswanathaReddy, G., Rambabu, G., DharmaSavarni, C. V. R., & Mittal, V. K. (2016, September). Multi-functional secured smart home. In *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 2629-2634). IEEE.

[18] Lunial, Hardik, et al. "Smart home automation ecosystem using internet-of-things." *AIP Conference Proceedings*. Vol. 3162. No. 1. AIP Publishing, 2025.

[19] Henkel, M., Haesler, S., Al-Najmi, H. K., Hessel, F., & Reuter, C. (2025). The House That Saves Me? Assessing the Role of Smart Home Automation in Warning Scenarios. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *9*(1), 1-32.

[20] Khan, A., Gupta, D., Dutta, M., & Lande, J. (2024, December). Securing Smart Homes: Machine Learning Solutions for IoT Cyber Threats. In *2024 International Conference on Innovation and Novelty in Engineering and Technology (INNOVA)* (Vol. 1, pp. 1-6). IEEE.

[21] Piyare, R., & Tazil, M. (2011, June). Bluetooth based home automation system using cell phone. In *2011 IEEE 15th international symposium on consumer electronics (ISCE)* (pp. 192-195). IEEE.

[22] Behera, A. R., Devi, J., & Mishra, D. S. (2015, October). A comparative study and implementation of real time home automation system. In *2015 International Conference on Energy Systems and Applications* (pp. 28-33). IEEE.

[23] Howedi, A., & Jwaid, A. (2016, December). Design and implementation prototype of a smart house system at low cost and multi-functional. In *2016 Future Technologies Conference (FTC)* (pp. 876-884). IEEE.

[24] Panwar, A., Singh, A., Kumawat, R., Jaidka, S., & Garg, K. (2017, July). Eyrie smart home automation using Internet of Things. In *2017 computing conference* (pp. 1368-1370). IEEE.

[25] Baraka, K., Ghobril, M., Malek, S., Kanj, R., & Kayssi, A. (2013, June). Low cost arduino/android-based energy-efficient home automation system with smart task scheduling. In *2013 Fifth international conference on computational intelligence, communication systems and networks* (pp. 296-301). IEEE.